A Research Proposal

on

Assessing the robustness of symmetric ciphers under proposed Bit Sum Attack

Submitted to

LOVELY PROFESSIONAL UNIVERSITY

In partial fulfillment of the requirements for the award of degree of

DOCTOR OF PHILOSOPHY (Ph.D.) IN COMPUTER APPLICATIONS/INFORMATION TECHNOLOGY

Submitted by:

Amandeep Bagga

Supervised by:

Dr. G. Geetha

LOVELY FACULTY OF TECHNOLOGY AND SCIENCES

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

1.0 INTRODUCTION (THE PROBLEM AREA TO BE INVESTIGATED)

1.1 Cryptanalysis

Any action that compromises the security of information is referred to as security attack. Security attack refers to Cryptanalysis. Cryptanalysis is the study of methods or techniques for obtaining the meaning of secret information which is encrypted, without access to the cryptographic system or the key used to encrypt the information. Typically, this includes finding method to get the secret key. In non-technical language, this is the practice of code breaking or cracking the code. "Cryptanalysis" is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols.

As cryptanalysis reveals weaknesses in various cryptosystems, cryptographers devise new and stronger cryptosystems in order to defeat all known methods of cryptanalysis.

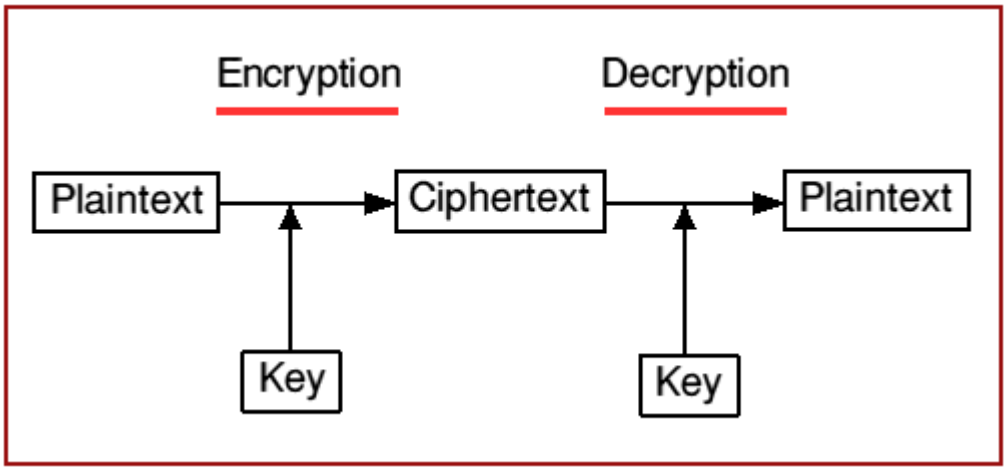

Fig. 1 General scheme of a cryptosystem [30]

1.2 Classification of Cryptanalysis Attacks

1.2.1 Classical Cryptanalysis

1.2.1.1 Ciphertext only Attack

In this type of attack, the cryptanalyst will try to get the plaintext, while having access only to the ciphertext i.e the coded text. This will include guessing the plaintext by using some techniques like frequency analysis etc.

Goal: Recover the original plaintext or plaintexts, to discover the deciphering key or find an algorithm for deciphering subsequent messages or ciphertext which was enciphered with the same key.

1.2.1.2 Known plaintext attack

In this type of attack, the cryptanalyst will have access to the ciphertext and corresponding plaintext also. So with this information cryptanalyst will try to find the correlation between two.

Goal: Recover the deciphering key or find an algorithm for deciphering subsequent messages (or the remaining plaintext) enciphered which use the same key.

1.2.1.3 Chosen plaintext attack

In this type of attack the cryptanalyst can encrypt the plaintext of his choice to produce and study the ciphertext.

Goal: Recover or discover the deciphering key or find an algorithm for deciphering subsequent messages or ciphertext which was enciphered with the same key.

1.2.1.4 Chosen Ciphertext attack

In this method of cryptanalysis, the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key.

Goal: In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

1.2.1.5 Adaptive Chosen Plaintext and Adaptive Chosen Ciphertext Attacks

In both types of adaptive attacks, the cryptanalyst takes advantage of the prior results. Cryptanalyst will be able to choose the further plaintexts or ciphertexts on the basis of the results he obtained from previous queries.

1.2.1.6 Rubber Hose Attack (Cryptanalysis)

Rubber hose attack/cryptanalysis is the process of extracting encryption keys from a user through the motivating use of a rubber hose. The process traditionally begins by tying the user to a post. You then strike the user with the rubber hose until he tells you the password or passphrase. Rubber hose cryptanalysis is the fastest method for key recovery from secure cryptosystems.

1.2.1.7 Frequency Analysis

Frequency analysis is a method of cryptanalysis and it is the study of the number of occurrences (frequency) of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

1.2.2 Cryptanalysis/Attack on Symmetric Algorithms

1.2.2.1 Differential cryptanalysis

Differential cryptanalysis is a type of chosen plaintext attack that seeks to discover a relationship between ciphertexts produced by two related plaintexts. It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm.

1.2.2.2 Linear cryptanalysis

Linear cryptanalysis is a type of known plaintext attack that requires access to large amounts of plaintext and ciphertext pairs encrypted with an unknown key. It focuses on statistical analysis against one round of decryption on large amounts of ciphertext.

1.2.2.3 Integral cryptanalysis

Integral cryptanalysis is type of cryptanalytic attack which is particularly applicable to block ciphers. It is based on substitution-permutation networks. It was originally designed by Lars Knudsen as a dedicated attack against Square, so is commonly known as the Square attack.

1.2.2.4 Statistical cryptanalysis

Statistical Cryptanalysis exploits probabilistic relationships among the plaintext, key and ciphertext to determine the key.

1.2.2.5 Mod-n cryptanalysis

"Mod n cryptanalysis is an attack applicable to block and stream ciphers. It is a form of partitioning cryptanalysis which exploits unevenness in how the cipher operates over equivalence classes modulo n".

1.2.2.6 Slide attack

Differential attack was successful on various strong block ciphers. To ward off the differential attack, an idea of increasing number of rounds to make weak ciphers stronger was quite prevalent. Slide attack was designed to deal with this prevailing idea. Slide attacks works on key schedule and find the weakness to break the cipher. For the working of slide attack, number of rounds in a cipher is irrelevant.

1.2.3 Other Cryptanalytic Attacks

1.2.3.1 Side Channel Attacks

Side channel attacks take the advantage of information acquired from physical implementation of the cryptosystems. It does not study the theoretical weaknesses in the algorithms, rather it studies the properties of the hardware used in encrypting or decrypting the information. For example, the acoustics, timing information, power consumption being used in processing of some particular calculations and even the sounds produced during the usage can provide the information required to deduce the information from the coded text.

1.2.3.2 Brute Force Attacks

This is the attack which tries all the possible combinations of keys to deduce the correct key. This kind of case happens when cryptanalyst is not able to find any weakness in the system, which reduces the search space. The length of the key will decide the practicality of this attack.

1.2.3.3 Meet-in-the-Middle Attack

Meet-in-the-middle attacks can be used against cryptographic algorithms that use multiple keys for encryption. The meet-in-the-middle attack is known plaintext attack; where cryptanalyst has access to both the plaintext and resulting ciphertext.

1.2.3.4 Birthday attack

The birthday attack is an attack that can discover collisions in hashing algorithms. It is based on the Birthday Paradox, which states that if there are 23 people in a room, the odds are slightly greater than 50% that two will share the same birthday.

1.2.3.5 Man in the Middle Attack

Man-In-The-Middle attack is the type of attack where attackers intrude into an existing connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data.

1.2.3.6 Differential Power Analysis

Differential power analysis is a class of attacks which analyses the power consumption in the semiconductor chip. After analysis, it applies the statistical computations on the information obtained power analysis.

1.2.3.7 Cache Attack

A technique that exploits the way in which Web browsers store recently viewed data could compromise privacy by allowing an attacker to check what sites a Net user has visited recently.

2.0 LITERATURE REVIEW

Literature review is based on Classification of Cryptanalytic Attacks and not on chronological order. This classification is explained in the introduction part, the literature review based on this classification is explained here.

2.1 Cryptanalytic Attacks

There are different attack types in cryptanalysis. Some facilitate the cryptographer's work, but may be unrealistic in certain situations. When wishing to cryptanalyze a cipher, it is important to know how the cipher is going to be used, because successfully cryptanalyzing it with an attack type, although remaining a good achievement, has little practical value if the cipher never gives away information required for this particular attack type. Ilya Saverchenko[1] has explained some classical ciphers and the types of attacks on them.

There are several kinds of attacks that one can use to break the ciphers:

1. Ciphertext-only Attack.

2. Known Plaintext Attack.

3. Chosen Plaintext Attack.

4. Chosen Ciphertext Attack

2.1.1 Ciphertext-only Attack.

The cryptanalyst intercepts one or more messages all encoded with the same encryption algorithm.

- This attack was tried on block cipher Akelerre [2] and proved that this cipher is weak even under the ciphertext only attack.
- In 2006, Elad Barkan, Eli Biham, Nathan Keller presented a very practical ciphertext-only cryptanalysis of GSM encrypted communication [3]
- Madryga is a blockcipher proposed in 1984 by W. E. Madryga . It was designed for efficient software implementation. Alex Biryukov and Eyal Kushilevitz has explained its cryptanalysis using ciphertext only attack[4].

2.1.2 Known Plaintext Attack.

Cryptanalyst will have access to the ciphertext and corresponding plaintext for some messages.

- Matsui has tried plaintext attack on DES cipher with different rounds[5]. Main results on the known –plaintext attack of DES cipher is as follows:
    - 8-round DES is breakable within 2^{21} known plaintexts in 40 seconds.
    - 12-round DES is breakable within 2^{33} known plaintexts in 50hours.
    - 16-round DES is breakable within 2^{47} known plaintexts faster than an exhaustive search for 56 key bits.
- Corfdir and Gilbert explained known plaintext attack[6] for FEAL-4 and FEAL-6. “It required about 1000 and 20000 plaintext blocks respectively and are based on correlation with linear functions. Using similar methods, he

found improved attack on FEAL-4 which requires only 200 known plain texts".

- Oorschot and Wiener had explained a known plain text attack on two key triple encryption[7].

2.1.3 Chosen Plaintext Attack.

The cryptanalyst has access to ciphertext for which he or she has the capability to specify the plaintext.

- Arroyo , Chengqing Li , Shujun Li ,Alvarez And Halang explained that how to break Chaotic Systems with chosen plain text attack[8]. "Chaotic systems have been broadly exploited through the last two decades to build encryption methods. Recently, two new image encryption schemes have been proposed, where the encryption process involves a permutation operation and an XOR like transformation of the shuffled pixels, which are controlled by three chaotic systems".

- In 2004, V.Bard demonstrated a weakness in SSL which potentially allows an attacker mounting a chosen-plaintext attack to gather information about the plaintext being encrypted[9]. In particular, the attack potentially enables an adversary to easily recover low-entropy information such as passwords or PINs that have previously been encrypted.

- Chardin and Marinier presented an attack of CMEA-I which requires less than 850 plaintexts in its adaptive version [10]. "This demonstrates that the improvements made over CMEA are ineffective to thwart such attacks and confirms that the security of CMEA (Cellular Message Encryption Algorithm) and its variants must be reconsidered from the beginning".

2.1.4 Chosen Ciphertext Attack.

In this type of attack the cryptanalyst collects the information by choosing the ciphertext and decrypt it with the help of unknown key. Cryptanalyst can gather some plaintexts and can deduce the correct key of the system.

- Bruce Schneier and Jonathan Katz[11] have explained a Chosen ciphertext attack against several e-mail encryption protocols.

- Jallad, Katz and Schneier[12] implemented chosen ciphertext attack against PGP and GnuPG. PGP and other e-mail encryption protocols.

To break modern cryptosystems, more sophisticated and complex techniques are used:

2.1.5 Rubber hose cryptanalysis

The actual meaning is "bypassing" of encryption via beating a person with a rubber hose until they provide their password.

- Chris L. Bresten[13] has discussed the growing popularity of rubber hose cryptanalysis and a solution to it. The solution is “deniable private key system”. The ideal deniable private key system would allow someone to encrypt multiple plaintexts into a single ciphertext, with separate keys. In the event of a rubber-hose attack, the holder of the keys can fork over an alternative key, yielding a plaintext that has been engineered to divert or confuse the attacker from the real secrets

2.1.6 Frequency Analysis

If the message had been encrypted with substitution cipher, and you want to decrypt this message, then you will find the solution with the help of frequency analysis. That means of sender has replaced the letters of the text with some other letter while encrypting, then those original letters will be recognised by analysing its frequency in the text. The frequency of the original letters will be passed to the encrypted text. To apply frequency analysis, one needs to prepare the frequency chart of that particular language, from which you can easily analyse the number of occurrences of particular letters.

- In 2009, Pedro Quaresma[14], had given frequency analysis of Portuguese Language. He presented the frequency of letters, digrams, trigrams, first letters, last letters, average length of the words, short words, and also the index of coincidence.

2.1.7 Kasiski Examination

Kasiski examination is a technique to attack polyalphabetic substitution ciphers to find the length of key, such as the Vigenère cipher.

- Ilya Saverchenko[1] has explained the kasiski examination of Vigenere Cipher.

2.1.8 Differential Cryptanalysis

The method searches for plaintext, ciphertext pairs whose difference is constant, and investigates the differential behaviour of the cryptosystem. Differential cryptanalysis is applicable to the iterated ciphers with a weak round function.

- Howard M. Heys[15] has explained Differential Cryptanalysis on SPN network.

2.1.9 Linear Cryptanalysis

- Matsui has explained Linear cryptanalysis on DES cipher with different rounds[5].
- Howard M. Heys[15] has explained Linear Cryptanalysis on SPN network.

2.1.10 Integral Cryptanalysis

- YONGJIN YEOM [16] has given some applications of integral cryptanalysis on block ciphers such as Camellia and Safer++. Also, shown that integral cryptanalysis can be interpreted as a special case of higher order differential attack.

2.1.11 Mod-n Cryptanalysis

- John Kelsey, Bruce Schneier and David Wagner [17] presented this attack with a mod 3 attack against an RC5 variant named RC5P. RC5P uses addition, not XOR.

2.1.12 XSL Attack

- Carlos Cid and GaÄetan Leurent[18] did the analysis of XSL algorithm. They presented strong evidence that, AES system of equations can’t be solved with the current form of XSL algorithm.

2.1.13 Slide Attack

- Soichi FURUYA[19] demonstrated applications of a slide attack to linear cryptanalysis, a DES variant case. In addition, we also show that

our enhancement enables to declassify the unknown primitive used in a block cipher. We test a block cipher, GOST, and show how to de-classify the hidden 4-bit substitution tables.

2.1.14 Birthday Attack

- Zhengjun Cao[20] explained a technique to launch the birthday attack against DES. The attack is entirely based on the simple key schedule and the relationship Li+1 = Ri in DES.

2.1.15 Man in the middle Attack

Man in the middle attack is well explained in [21]

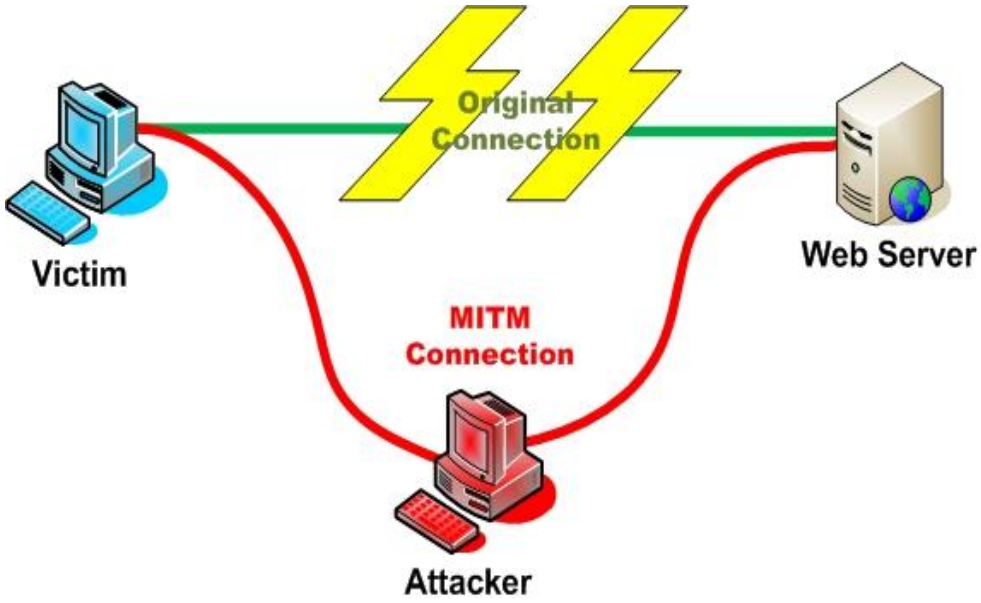

Fig. 2 Illustration of man-in-the-middle attack [31]

2.1.16 Differential Power Analysis

- Paul Kocher, Joshua Jaffe and Benjamin Jun [22] examined specific methods for analysing power consumption measurements to find secret keys from tamper resistant devices. They also discussed approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

2.1.17 Side Channel attack

- John Kelsey, Bruce Schneier, David Wagner and Chris Hall [23] presented side-channel attacks. This attack was demonstrated against three product ciphers:
  - timing attack against IDEA
  - processor flag attack against RC5
  - Hamming weight attack against DES.

2.1.18 Cache Attack

- Anne Canteaut, Cedric Lauradoux and Andre Seznec [24] given the basic understanding of cache attack. He found that due to the structure of the cache memory, such an attack against AES enables to recover the most significant bits of each key byte.

2.1.19 Brute Force Attack

- Brute force attack is very well explained in [25]

3.0 OBJECTIVES /SCOPE OF THE STUDY

The objective of our study is to investigate a chosen plaintext attack on symmetric ciphers. Tiny Encryption Algorithm, Fast Encryption Algorithm, Blowfish, Twofish, AES, Threefish will be examined using the algorithm we have devised.

Based on our method of cryptanalysis, we hope to grade the strength of above symmetric key algorithms. We hope to have savings in the key space search over brute force. We also hope to bring out some interesting properties of symmetric algorithms under study.

4.0 PROPOSED METHODOLOGY

4.1 Basis of our Algorithm

Let us consider that we have a cryptographic algorithm (cipher) for which the key consists of zeros and ones. Without loss of generality, suppose the key is of length 64 bits. A brute force attack would test 2^64 keys in total for a worst case scenario. Now, if we were somehow able to determine the bitsum of the key (that is, the numbers of ones present), the keyspace would be greatly reduced.

The worst case scenario here would be 32 ones, for which we would have 64C32 (64 choose 32) possible keys. So how could we determine the bitsum of the key? Obviously, this is the difficult part.

We propose investigating a chosen plaintext attack. The hope would be that there is a specific message for which the bitsum of the ciphertext correlates with the bitsum of the key. The correlation would likely not be perfect, so a suggested range of values for the bitsum of the key may be produced. Still, this would be a great savings over brute force. This is the basis of our algorithm that will be used to investigate the strength of Symmetric ciphers.

4.2 Selection of the Symmetric Ciphers to check their Cryptographic Strength against the proposed attack

The Following are the algorithms chosen for applying this attack. The algorithms are chosen because of their popularity and their strength against the attacks till date.

4.2.1 Tiny Encryption Algorithm

Tiny Encryption Algorithm (TEA) is a block cipher . It is notable for its easy description and implementation. This algorithm was designed by David Wheeler and Roger Needham [26] at the Computer Laboratory of Cambridge University. "TEA operates on 64-bit blocks and uses a 128-bit key. It has a Feistel structure with a suggested 64 rounds. Typically implemented in pairs termed cycles. It has an extremely simple key schedule, mixing all of the key material in exactly the same way for each cycle".

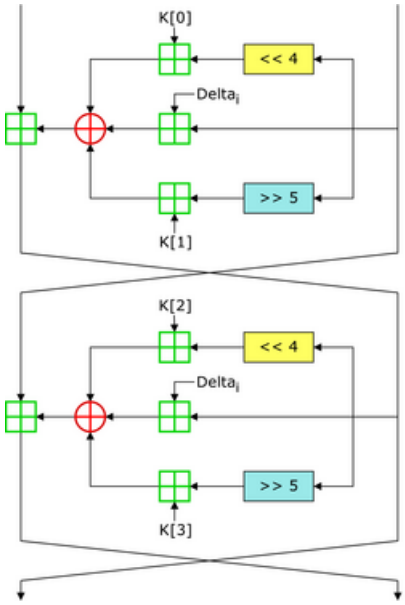

Fig. 3 Two Feistel rounds (one cycle) of TEA [32]

4.2.2 Fast data Encipherment Algorithm (FEAL)

FEAL (the **F**ast data **E**ncipherment **AL**gorithm) is a fast algorithm. It was designed and proposed as an alternative for Data Encryption Standard (DES). It is Feistel based block cipher. It was first published by Akihiro Shimizu and Shoji Miyaguchi[27] from NTT in 1987. The cipher is prone to several forms of cryptanalysis, and has performed like a catalyst in the discovery of differential and linear cryptanalysis.

"There have been several different revisions of FEAL, though all are Feistel ciphers, and make use of the same basic round function and operate on a 64-bit block. One of the earliest designs is now termed FEAL-4, which has four rounds and a 64-bit key".

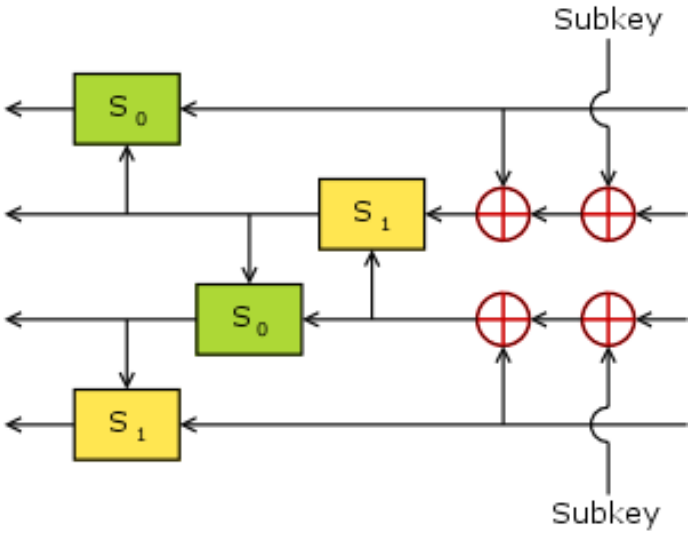

Fig. 4 The FEAL Feistel function[33]

4.2.3 Blowfish Algorithm

Blowfish is a symmetric cipher that can be effectively used for encryption and safeguarding of data. It is also a block cipher that takes a key of variable-length, from 32 bits to 448 bits, making it ideal for securing data. This cipher was designed as a fast, free alternative to existing encryption algorithms by Bruce Schneier [28] in 1993.

"Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits".

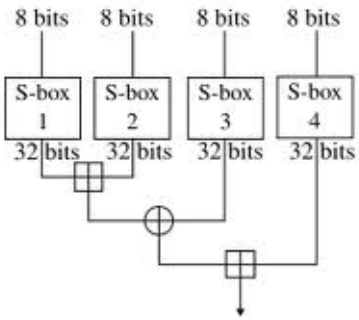

Fig. 5 The round function (Feistel function) of Blowfish [34]

4.2.4 Twofish Algorithm

Twofish is a block cipher designed by John Kelsey, Bruce Schneier, David Wagner, Niels Ferguson, Chris Hall and Doug Whiting[29].

- Twofish is symmetric algorithm with 128 bit block and key of length upto 256 bits. It is good for software running on small devices as well as good for

hardware like embedded chips. Twofish algorithm also uses Feistel structure as DES does.

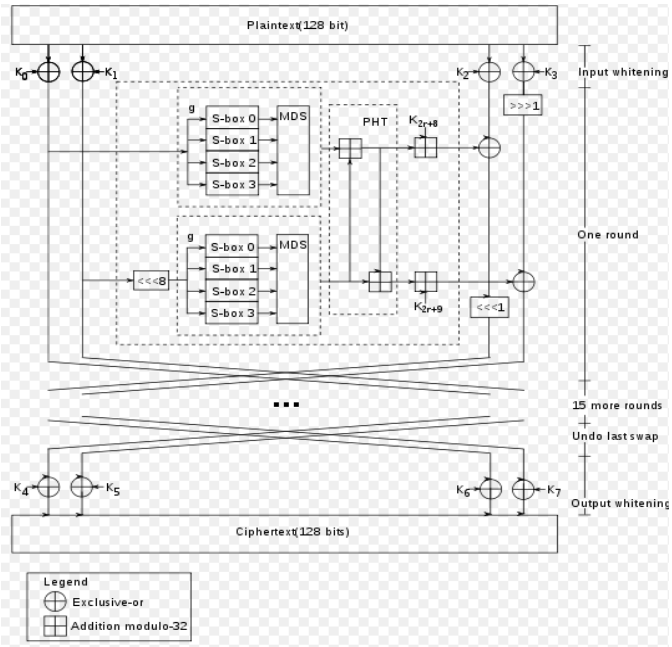

Fig. 6 The Twofish Algorithem [35]

4.3 Methodology for attacking the Ciphers

For cipher under investigation, we would write a program to encipher a fixed message M with 100 different keys and then calculate the correlation of the bitsums of the ciphertexts produced with the bitsums of the corresponding keys. This would all be inside a loop that changes the message. As we cycle through as many messages as possible, we will keep track of which message yields the best correlation between bitsums of ciphertext and key. This method will be followed for all symmetric ciphers under examination and conclusions drawn.

References:

[1] I. Saverchenko.(2005) Classical Cryptography. [online]. Available: http://www14.informatik.tu-muenchen.de/konferenzen/Jass05/courses/1/papers/saverchenko_paper.pdf

[2] L. R. Knudsen, V. Rijmen, “Two Rights Sometimes Make a Wrong”, *in Proc.* SAC, 1997, pp. 213—223

[3] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", *in Proc. CRYPTO*, 2003, pp.600-616.

[4] A. Biryukov and E. Kushilevitz, "From Differential Cryptoanalysis to Ciphertext-Only Attacks", *in Proc. CRYPTO*, 1998, pp.72-88.

[5] M. Matsui, "Linear Cryptoanalysis Method for DES Cipher", *in Proc. EUROCRYPT*, 1993, pp.386-397.

[6] A. Tardy-Corfdir and H. Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6", *in Proc. CRYPTO*, 1991, pp.172-181.

[7] P.C.V. Oorschot and M.J. Wiener, "A Known Plaintext Attack on Two-Key Triple Encryption", *in Proc. EUROCRYPT*, 1990, pp.318-325.

[8] D. Arroyo, C. Li, S. Li, G. Álvarez, and W.A. Halang, "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm", presented at CoRR, 2007.

[9] G. Bard,” The vulnerability of ssl to chosen-plaintext attack”. Cryptology ePrint Archive, Report 2004/111, 2004.

[10] T. Chardin and R. Marinier, "An Adaptive Chosen-plaintext Attack of the Improved Cellular Message Encryption Algorithm", *in Proc.* I. J. Network Security, 2009, pp.173-179.

[11] J. Katz and B. Schneier, “A chosen Ciphertext Attack Against Several E-Mail Encryption Protocols” *in Proc.* 9th USENIX Security Symposium, 2000, pp. 241-246.

[12] K. Jallad, J. Katz, and B. Schneier, "Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG", *in Proc.* ISC, 2002, pp.90-101.

[13] C. L. Bresten. (2009) A General Framework for a Deniable Private Key

Chaotic Cryptosystem. [Online]. Available: http://compmath.files.wordpress.com/2009/02/cbfreport.pdf

[14] P. Quaresema. (2008) Frequency Analysis of the Portuguese Language. [Online]. Available: http://www.mat.uc.pt/~pedro/cientificos/Cripto/CISUC-TR200803.pdf

[15] Howard M. Heys, "A Tutorial on Linear and Differential Cryptanalysis", Cryptologia, Volume 26 Issue 3, July 2002 , 189–221.

[16] Y. Yeom, "Integral Cryptanalysis and Higher Order Differential Attack", Trends in Mathematics, Information Center for Mathematical Sciences, Volume 8, Number 1, June, 2005, Pages 101-118.

[17] J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, with Applications Against RC5P and M6", in Proc. FSE, 1999, pp.139-155.

[18] C. Cid and G. Leurent, "An Analysis of the XSL Algorithm", in Proc. ASIACRYPT, 2005, pp.333-352.

[19] S. Furuya, "Slide Attacks with a Known-Plaintext Cryptanalysis", in Proc. ICISC, 2001, pp.214-225.

[20] Z. Cao, "How to Launch A Birthday Attack Against DES", Cryptology ePrint Archive: Report 2008/288, 2008.

[21] A. Menezes, P. VanOorschot, S. Vanstone (1996) Handbook of Applied Cryptography 500, 642.

[22] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", in Proc. CRYPTO, 1999, pp.388-397.

[23] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers", in Proc. ESORICS, 1998, pp.97-110.

[24] A, Canteaut , C. Lauradoux , A.Seznec, "Understanding Cache Attacks", INRIA Open Archive, Research Report, 2006.

[25] B. Scheneir (1996) *Applied Cryptography* 151-152, 154-155.

[26] D.J. Wheeler and R.M. Needham, "TEA, a Tiny Encryption Algorithm", *in Proc.* FSE, 1994, pp.363-366.

[27] A.Shimizu, S. Miyaguchi, "Fast Data Encryption Algorithm FEAL", *In Proc* EUROCRYPT'87, pp.267-278, 1987.

[28] B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish.)", *In Proc* FSE, 1993, pp.191-204.

[29] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C." Hall. Twofish: a 128-bit block cipher", *In Proc*. First Advanced Encryption Standard (AES) Conference, 1998.

[30] http://www.queen.clara.net/pgp/AU265.html

[31] https://www.owasp.org/index.php/Man-in-the-middle_attack

[32] http://bechtsoudis.com/cryptography/tea-cipher-on-arms-isa/

[33] http://it.wikipedia.org/wiki/FEAL

[34] http://www.search.com/reference/Blowfish_(cipher)

[35] http://www.ask.com/wiki/Twofish